CLAIMS

1. A method for defining sets of encryption keys from a key matrix, comprising:

receiving at least one parameter representing a characteristic of the key matrix;

using the parameter and an error-correcting code, defining plural sets of keys; and

assigning at least some sets of keys to at least some respective devices.

2. The method of Claim 1, wherein the error-correcting code is a Reed-Solomon code.

3. The method of Claim 1, wherein each set of keys represents a set of key indices in the key matrix, each key index being associated with a respective key.

4. The method of Claim 1, wherein the receiving act includes receiving at least a row parameter "N" representing the number of rows in the key matrix and a column parameter "n" representing the number of columns in the key matrix, and the method further includes:

using an error-correcting code having a Hamming distance "d" that minimizes key overlap between sets of keys.

5. The method of Claim 4, wherein the error-correcting code defines the sets of keys using a total predefined number "T" of sets.

6. The method of Claim 1, wherein the error-correcting code is associated with a compact generating function and the method further comprises storing the compact generating function and an index of one and only one stored set of keys, whereby no set of keys other than the index of the stored set of keys need be stored in that sets of keys can be regenerated using the compact generating function and the index of the stored set.

7. The method of Claim 6, wherein the compact generating function is a generating matrix G, and the method further comprises transforming the compact generating function G to have a non-systematic row assignment.

8. The method of Claim 1, wherein the error-correcting code generates vectors over an alphabet having symbols, and the method further comprises renaming at least one symbol based on a pseudorandom permutation.

9. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for defining, based on at least one error-correcting code, plural sets of keys useful by respective devices for decrypting encrypted content.

10. The device of Claim 9, wherein each set represents a set of coordinates in a key matrix.

11. The device of Claim 9, further comprising logic means for associating plural sets of keys with respective devices.

12. The device of Claim 9, wherein the error-correcting code is a Reed-Solomon code.

13. The device of Claim 9, wherein the means for defining includes:

logic means for receiving at least a row parameter "N" representing the number of rows in the key matrix and a column parameter "n" representing the number of columns in the key matrix;

logic means for using an error-correcting code having a Hamming distance "d" that minimizes key overlap between sets of keys.

14. The device of Claim 13, wherein the error-correcting code defines the sets of keys using a total predefined number "T" of sets.

15. The device of Claim 9, wherein the error-correcting code is associated with a compact generating function, and the device further comprises logic means for storing the compact generating function and an index of a stored set of keys, whereby no sets of keys need be stored in that sets of keys can be regenerated using the compact generating function and the index of the stored set.

16. The device of Claim 15, wherein the compact generating function is a generating matrix G, and the device further comprises logic means for transforming the generating matrix G to have a non-systematic row assignment.

17. The device of Claim 9, wherein the error-correcting code generates vectors over an alphabet having symbols, and the device further comprises logic means for renaming at least one symbol based on a pseudorandom permutation.

18. A computer programmed with instructions to cause the computer to execute method acts including:

receiving, as input, at least a number "n" representing a number of columns in a key matrix and a number "N" representing a number of rows in the key matrix, each position in the key matrix being definable by a respective index, each index being associated with a respective key useful by a decryption device for decrypting encrypted content;

defining, based at least in part on the input, plural sets of keys using a non-random function.

19. The computer of Claim 18, wherein the non-random function is an error-correcting code.

20. The computer of Claim 19, wherein the error-correcting code is a Reed-Solomon code.

21. The computer of Claim 18, wherein the method executed by the computer further includes assigning at least some sets of keys to at least some respective devices.

22. The computer of Claim 19, wherein the error-correcting code is associated with a generating matrix G, and the method executed by the computer further comprises storing the generating matrix G and an index of a stored set of keys, whereby no set of keys other than the index of the stored set of keys need be stored in that sets of keys can be regenerated using the generating matrix G and the index of the stored set.

23. The computer of Claim 22, wherein the method executed by the computer further comprises transforming the generating matrix G to have a non-systematic row assignment.

24. The computer of Claim 18, wherein the error-correcting code generates vectors over an alphabet having symbols, and the method executed by the computer includes renaming at least one symbol based on a pseudorandom permutation.

25. The method of Claim 4, wherein the error-correcting code is a linear code.

26. The device of Claim 9, wherein the error-correcting code is a linear code.

27. The computer of Claim 19, wherein the error-correcting code is a linear code.